ORIGINAL

PATENT AF

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Michael WRAY	)	On appeal to the Board of Patent Appeals and Interferences
Application No.: 09/732,948	)	Group Art Unit: 2134
Filed: December 7, 2000	)	Examiner: Norman M. Wright
For: "Electronic Certificate"	)	Date: January 4, 2007

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the office action mailed on August 24, 2006 for the above identified patent application. The notice of appeal was timely filed on November 21, 2006. This appeal brief is timely and no appeal brief fee need be paid because this is a reinstated appeal. M.P.E.P. § 1204.01.

REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of the Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal, other than the appeal filed in this application by a notice mailed on January 26, 2006. The present appeal is the **second** in this application. The earlier appeal resulted in a re-opening of prosecution and a non-final office action mailed on August 24, 2006. The Examiner rejected the pending claims on exactly **the same grounds** as in the final action that led to the first appeal. In addition, the Examiner added an **alternative rejection** of the same claims that relied on a reference that had been cited in the first office action but in none of the succeeding actions until the last one, the office action of August 24, 2006. In response, the Appellant reinstated the appeal by the notice mailed on November 21, 2006.

STATUS OF CLAIMS

Claims 1-11 and 14-30 are currently pending. Claims 12 and 13 were cancelled in the amendment filed on December 13, 2004. Claims 1-11 and 14-30 are the subject of this appeal and are reproduced in the accompanying claims appendix.

STATUS OF AMENDMENTS

No amendment after final rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates to electronic certificates that delegate an attribute from an issuer to a subject and are signed by the user. Specification at page 1, lines 5-6. An "attribute" is any capability, characteristic or authorization that can be associated with the subject. *Id.* at page 1, lines

8-11. "Delegation" means to bestow an attribute by an issuer of a certificate to the subject named in the certificate. *Id.* at page 1, lines 13-14.

Electronic certificates are useful for controlling access to electronic resources. They are useful for facilitating electronic commerce.

The prior art to this application, the "aapa," discloses the issuance of electronic certificates to subjects who may then in turn issue electronic certificates to further subjects if given that authority, and the proving of a trusted chain of delegations of authorization so that a given subject may be authorized to use an electronic resource. *Id.* at page 1, line 23 to page 5, line 31.

The aapa provides for issuance of certificates only when any prior conditions regarding the attribute to be possessed by the subject have been proved to the satisfaction of the certificate issuer. This is an unconditional issuance because the issuer has been satisfied that the prior conditions have been met and therefore the issuer issues the certificate. Having to satisfy the *issuer* can significantly hamper the issuing of certificates. *Id.* at page 6, lines 4-8.

The standard VALIDITY field of aapa certificates is, in effect, a condition carried by the certificate. It could include data about, for example, the date range identifying the period over which the certificate is valid. This is *a condition directed at the validity of the certificate itself and does not define an attribute required of a particular subject. Id.* at page 6, line 28 to page 7, line 8.

The invention, as claimed in claims 1-10, generally provides "computer-readable medium storing an electronic certificate data structure comprising content data specifying an attribute delegation from an identified issuer to a certificate subject, and an electronic signature of said issuer for confirming the content data; wherein the content data includes a condition *requiring that a particular subject must have a particular attribute in order for the delegation to be valid*" (emphasis added.) This aspect of the invention is

generally directed to electronic certificates that contain subject-directed conditions that *must* be found to be true in respect of the subject of the certificate before that subject can be taken as having been delegated the attribute specified in the certificate. *Id.* at page 8, lines 8-15 and Figure 5. These certificates may be called conditional electronic certificates. *Id.* at page 8, lines 15-16.

The difference may be illustrated by Figures 2 and 5 of the drawings for this application. Figure 2, showing a diagram of an attribute certificate of the "prior art," is reproduced below:

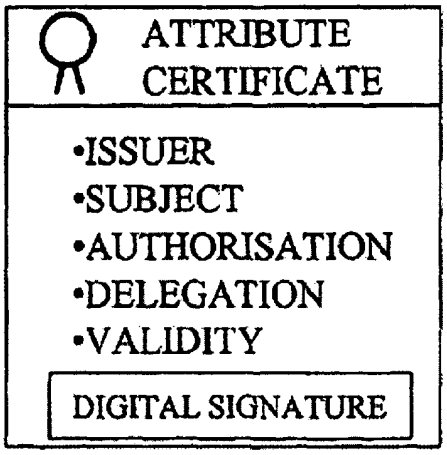


Figure 2

(PRIOR ART)

Figure 5, showing a diagram of a conditional certificate "embodying the present invention," is reproduced below:

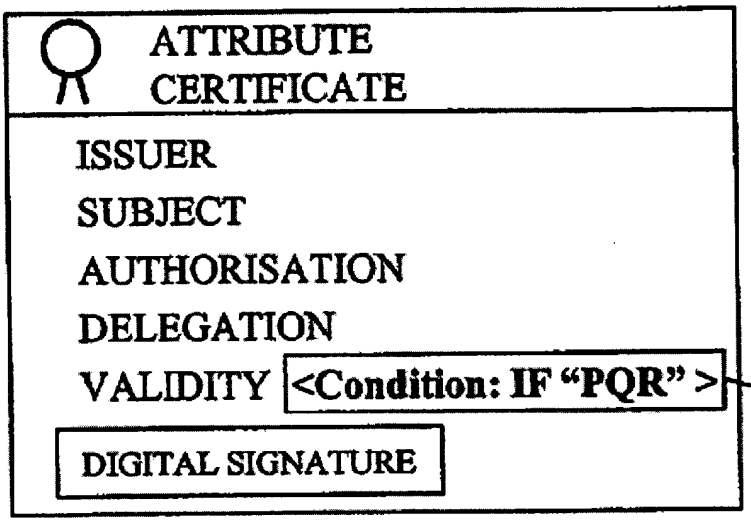


Figure 5

The specification provides an example of a condition in the content data of a conditional electronic certificate. The "condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid" to be satisfied is that a principal (employee Z) is an authorized buyer of department Y of company X. A chain of aapa electronic certificates can provide a trust chain between issuer SELF and employee Z but this cannot independently establish that employee Z has the attribute or qualification of being an authorized buyer. A conditional electronic certificate of the kind disclosed in this application will require the subject (employee Z in this example) to have a specified qualification attribute. Even though all employees of department Y may have the attribute "authorized buyer of department Y" applied to them to prove they are the subjects of their certificates the certificates would still *require the subject to have a specified qualification*. The specified qualification could be provided, for example, by a trusted third party or by a training section TS of the department Y of the company X to establish that the employee X has the requisite qualification. The certificate will then prove a trusted relationship so that employee X may have access to the desired capability or

attribute. *See generally id.* at page 17, line 19 to page 18, line 7. More than one attribute required of a subject, linked in a logical order such as AND, OR, and NOT, can be included in a conditional certificate. *Id.* at page 8, lines 18-22.

Claims 11 and 14-18 are directed to apparatus for generating such conditional electronic certificates. Claims 19-24 are directed to reduction engines (*see* Figures 11-13) for verifying the existence of a trust chain of justified attribute delegations that comprises a trust-chain branch control arranged to require the trust-chain verifier to establish a branch of the trust chain when a conditional certificate is encountered. Claims 25-30 are directed generally to a trust chain discovery engine (*see* Figures 6 and 11-13) for finding a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject that comprises a trust-chain branch control arranged to require the trust-chain builder to seek to build a branch of the trust chain when a conditional certificate is encountered.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1-11 and 14-30 are patentable under 35 U.S.C. 103(a) in view of Appellant's admitted prior art (the "aapa")?

Issue 2: Whether Claims 1-11 and 14-30 are patentable under 35 U.S.C. 103(a) over the aapa in view of U.S. patent 6,658,568 to Ginter, et al. ("Ginter")?

ARGUMENT

I. Claims 1-11 and 14-30 Are Patentable under 35 U.S.C. § 103(a) in View of the Aapa

In the Office Action of August 24, 2006, the Examiner rejected claims 1-11 and 14-30 under 35 U.S.C. 103(a) as being obvious over the aapa.

The Appellant respectfully disagrees with the conclusions of the Examiner with regard to the teaching of the cited prior art and submits that the aapa does not teach or suggest all of the claim limitations of the rejected claims. Therefore, the Appellant submits that the Examiner has not established a *prima facie* case of obviousness based on the aapa, and the rejection of claims 1-11 and 14-30 based on the aapa should be overturned on appeal.

Claim 1

Claim 1 requires:

> [a] computer-readable medium storing an electronic certificate data structure, the data structure comprising:
>
> content data specifying an attribute delegation from an identified issuer to a certificate subject, and
>
> an electronic signature of said issuer for confirming the content data;
>
> wherein the content data includes a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid.

The Examiner held that these limitations are all taught in the aapa except "[n]ot explicitly taught is the certificate being stored in a memory," which he held to be obvious. Final office action at page 2, line 17 to page 3, line 8.

The Examiner held that the limitation "the content data includes a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid" is disclosed in the aapa because, as he asserts on page 3 of the final Office Action, "a condition in aapa is that the particular party must be able to

respond to the challenge-response transaction by knowing the key pair used to encrypt the data." However, the aapa does not disclose a certificate with "content data" that has *a conditional association of an attribute with a subject* in order for the delegation to be valid.

The Appellant notes that the aapa certificate has a specified certificate subject (SUBJECT in Figure 2) to whom a specified particular attribute (AUTHORISATION) is being passed by the certificate. A party R receiving the aapa certificate accepts that the specified certificate subject now has the particular attribute specified in the aapa certificate (assuming that the party R trusts the party signing the certificate). This acceptance is *unconditional.*

When a party X claims that the aapa certificate proves that party X has a particular attribute, party R can choose simply to accept that party X is the aapa certificate subject, or party R can choose to check the identity of party X (see page 3, lines 4-7 of the specification). Party R can effect this check in many ways, one of which is by effecting a challenge-response exchange. Such a check on the identity of party X is a completely separate issue from what attribute delegation is effected by the aapa certificate.

The aapa certificate does not require the certificate subject to prove its identity (by a challenge-response exchange). Proof of identity is merely at the discretion of the party receiving the certificate. The "subject" public key in the aapa certificate merely implicitly corresponds to a condition indicating that a particular subject can have a particular attribute (possess the private key matching the subject public key) in order for the delegation (the certificate overall) to be valid. However, the aapa certificate may be valid even if the subject does not have the particular attribute (if the receiving party does not check the attribute through a challenge-response transaction).

Accordingly, the aapa fails to disclose or suggest a computer-readable medium storing an electronic certificate data structure with content data including a *"condition requiring that a particular subject must have a particular attribute in order for the delegation to be*

valid", as recited in claim 1. Claim 1 requires that the validity of the attribute delegation to the certificate subject is to be conditional on the subject having a particular attribute. This is not taught by the aapa. The subject matter of claim 1 therefore is not taught or suggested by the aapa.

As the M.P.E.P. points out, at Section 2143,

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Before considering motivation and reasonable expectation of success, the prior art reference must "teach or suggest all the claim limitations." As noted above, the aapa does not teach or suggest all of the claim limitations. The Appellant therefore submits that claim 1 is patentable over aapa because the Examiner has not made out a *prima facie* case of obviousness based on the aapa. The rejection of this claim over the aapa should be withdrawn.

Claim 11

Claim 11 requires:

> [a]pparatus for generating an electronic certificate data structure, the apparatus comprising:
> a data handling arrangement for assembling content data specifying an attribute delegation from an identified issuer to a certificate subject, and

including a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid; and

a signature arrangement for generating an electronic signature of said issuer over said content data.

The above arguments show that the aapa fails to disclose or suggest an apparatus as recited in claim 11, and in particular comprising a data handling arrangement for *"including a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid"*. At least in view of the above, the Appellant submits that claim 11 is patentable over the aapa and the rejection of this claim over the aapa should be withdrawn.

Claim 19

Claim 19 requires:

[a] reduction engine for verifying the existence of a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine comprising:

a trust-chain verifier for combining justified attribute delegations to form said trust chain, at least one said attribute delegation being justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain verifier to establish a branch of said trust chain upon the trust-chain verifier

using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

The above arguments show that the aapa fails to disclose or suggest a reduction engine as recited in claim 19, and in particular comprising a trust-chain branch control arranged to *"require the trust-chain verifier to establish a branch of said trust chain upon the trust-chain verifier using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid."* At least in view of the above, the Appellant submits that claim 19 is patentable over the aapa and the rejection of this claim over the aapa should be withdrawn.

Claim 25

Claim 25 requires:

[a] trust chain discovery engine for finding a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said discovery engine comprising:

a trust-chain builder for seeking to build up said trust chain using justified attribute delegations at least one of which is justified on the basis

of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain builder to seek to build a branch of said trust chain upon the trust-chain builder using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

The above arguments show that the aapa fails to disclose or suggest a trust chain discovery engine as recited in claim 25, and in particular comprising a trust-chain branch control arranged to *"require the trust-chain builder to seek to build a branch of said trust chain upon the trust-chain builder using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid."* At least in view of the above, the Appellant submits that claim 25 is patentable over the aapa and the rejection of this claim over the aapa should be withdrawn.

Claims 2-9, 14-17, 20-23 and 26-30

Claims 2-9 depend directly or indirectly on claim 1; claims 14-17 depend directly or indirectly on claim 11; claims 20-23 depend directly or indirectly on claim 19; and

claims 26-30 depend directly or indirectly on claim 25. The Appellant respectfully submits that at least in view of their dependency on claims 1, 11, 19 or 25, claims 2-9, 14-17, 20-23 and 26-30 are patentable over the aapa. M.P.E.P. § 2143.03 ("If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)").

II. Claims 1-11 and 14-30 Are Patentable Under 35 U.S.C. § 103(a) Over the aapa in View of Ginter

In the Office Action of August 24, 2006, the Examiner rejected claims 1-11 and 14-30 in the alternative under 35 U.S.C. § 103(a) as being obvious over the aapa in view of Ginter. The Appellant respectfully disagrees. A *prima facie* case of non-obviousness has not been made out and this rejection should be withdrawn.

This is not the first time that Ginter has made an appearance in the prosecution history of this application. Thus, claims 1-13 were rejected as being anticipated by Ginter in the first and non-final office action mailed on October 6, 2004. In an amendment filed on December 13, 2004, Appellant amended claims 1-11 to address, *inter alia*, 35 U.S.C. §§ 101 and 112 concerns (e.g., "certificate" became "a computer-readable memory storing an electronic certificate" in claims 1-10 and "apparatus for generating a certificate" became "apparatus for generating an electronic certificate" in claim 11), cancelled claims 12 and 13, and argued that the subject matter of claims 1-11 was not anticipated by Ginter.

In response, the final office action mailed on April 21, 2005 made no mention of Ginter and instead rejected some of the claims (claims 1-9, 11, 14-17, 19-23, and 25-29) under 35 U.S.C. § 103(a) as being obvious over the aapa (claims 1-11 and 14-30 also were rejected as being indefinite). The Appellant filed a

request for continued examination and response to the final office action on August 8, 2005. No discussion of Ginter was necessary. The final office action of December 2, 2005 also did not mention Ginter. The appeal brief filed on April 24, 2006 therefore did not mention Ginter.

Ginter reappeared in the non-final office action mailed on August 24, 2006, from which this appeal lies: "[a]lternatively, if the conditional access attribute in AAPA is not what is claimed and described the inventive concept then [sic], the examiner recites [Ginter], as evidence for a conditional access attribute (see figs. 42, 44-45c, 50 and 51a-51c, (504), and cols. 30 line 1-53 et seq., cols 81-83)." Non-final office action mailed on August 24, 2006, at pp. 4-5.

Specifically, Ginter is cited to support the proposition that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to modify AAPA with the type of digital certificate that has the conditional control attributes as recited in [Ginter]." *Id.* at page 5. The Examiner claims that one of ordinary skill in the art would have been motivated to perform such a modification because Ginter "teaches a trusted infrastructure and system for creating and administrating certificates digitally signed by a trusted authority that provides conditional access attributes/information that requires the recipient to verify that he has authorization to use said information for enhanced security and scalability (abs., summary, and col. 12-13)." *Id.*

It will be noted that the Examiner alternatively cites to 344 lines of text (col. 30, lines 1-53 and cols. 81-83) and 1,236 lines of text (col. 4, line 46 to col. 13, line 50 (the summary, which includes cols. 12 and most of 13) of Ginter as teaching a "conditional access attribute." Citing such large blocks of text indicates that the Examiner does not

know specifically where Ginter teaches the features in question and is using a shotgun approach that will hopefully hit the target.[1]

Claim 1

A careful reading of the cited portions of Ginter, however, shows that Ginter discloses nothing beyond electronics certificates that may comprise "an expiration field 560(3) specifying when the digital certificate expires" (column 84, line 11). Such expiry date of the certificate is clearly distinct from "a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid" as recited in claim 1. There is nothing in Ginter that could be understood as teaching the inclusion in a certificate of requirements that must be satisfied by the receiver of the certificate (i.e., the certificate subject). The certificates of Ginter simply contain a field that causes them to expire at a certain date, with no input from or dependence on a receiver of the certificate.

The electronic certificates of Ginter are used for certifying the attributes of a subject, for example for "certifying the consumer's identity, age, or the like" (column 18, lines 18-20). Ginter does nowhere teach nor suggest an electronic certificate validated by an attribute of a subject. If the Examiner disagrees, Appellant respectfully request him to clearly and specifically point out in his reply brief where Ginter discloses the claimed feature in accordance with 37 C.F.R. 1.104(c)(2).

[1] The Examiner has not followed the requirement of 37 C.F.R. § 104(c)(2), which states: "[i]n rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, ***the particular part relied on must be designated as nearly as practicable***. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified." [Emphasis supplied.]

Claim 11

The above arguments also apply to show that Ginter fails to teach or suggest an "apparatus for generating an electronic certificate data structure, the apparatus comprising: a data handling arrangement for assembling content data specifying an attribute delegation from an identified issuer to a certificate subject, and including a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid; and a signature arrangement for generating an electronic signature of said issuer over said content data," as recited in claim 11, and can therefore not be deemed to render claim 11 unpatentable.

Claim 19

Likewise, Ginter fails to teach or suggest "[a] reduction engine for verifying the existence of a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine comprising: a trust-chain verifier for combining justified attribute delegations to form said trust chain, at least one said attribute delegation being justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and a trust-chain branch control arranged to require the trust-chain verifier to establish a branch of said trust chain upon the trust-chain verifier using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer," as recited in claim 19, and can therefore not be deemed to render claim 19 unpatentable.

Furthermore, Ginter fails to teach or suggest "[a] trust chain discovery engine for finding a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said discovery engine comprising: a trust-chain builder for seeking to build up said trust chain using justified attribute delegations at least one of which is justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and a trust-chain branch control arranged to require the trust-chain builder to seek to build a branch of said trust chain upon the trust-chain builder using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer," as recited in claim 25, and can therefore not be deemed to render claim 25 unpatentable.

Claims 2-9, 14-17, 20-23 and 26-30

Claims 2-9 depend directly or indirectly on claim 1; claims 14-17 depend directly or indirectly on claim 11; claims 20-23 depend directly or indirectly on claim 19; and claims 26-30 depend directly or indirectly on claim 25. The Appellant respectfully submits that at least in view of their dependency on claims 1, 11, 19 or 25, claims 2-9, 14-17, 20-23 and 26-30 are patentable over the aapa in view of Ginter.

CONCLUSION

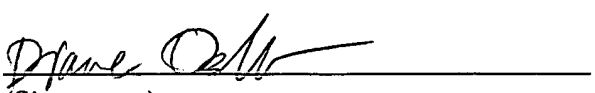
For the reasons advanced above, the Appellant respectfully contends that claims 1-11 and 14-30 are patentable over the aapa and separately over the aapa in view of Ginter. The Appellant respectfully submits that the Board should reverse and withdraw all rejections of the claims pending in the instant application.

* * *

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed or the petition for extension of time accompanying this brief is incorrect in stating or paying for the amount of time requested, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this Appeal Brief timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 4, 2007.

Diane Osollo
(Name of Person Transmitting)


(Signature)

January 4, 2007
(Date)

Respectfully submitted,

R. Dabney Eastham
Attorney for Appellant
Reg. No. 31,247
LADAS & PARRY LLP
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
reastham@ladas.com

1. A computer-readable medium storing an electronic certificate data structure, the data structure comprising:

content data specifying an attribute delegation from an identified issuer to a certificate subject, and

an electronic signature of said issuer for confirming the content data;

wherein the content data includes a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid.

2. A computer-readable medium according to claim 1, wherein said certificate subject is generically any subject whereby said attribute is delegated to any subject capable of showing said condition to be satisfied, the particular subject of said condition being explicitly identified in the content data.

3. A computer-readable medium according to claim 1, wherein said certificate subject is specifically identified in the content data.

4. A computer-readable medium according to claim 3, wherein said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

5. A computer-readable medium according to claim 3, wherein said particular subject is explicitly identified.

6. A computer-readable medium according to claim 1, including multiple said conditions in predetermined logical relationship.

7. A computer-readable medium according to claim 6, wherein said logical relationship is not explicitly but is explicitly stated.

8. A computer-readable medium according to claim 6, wherein said logical relationship is not explicitly but is implicitly an AND relationship.

9. A computer-readable medium according to claim 1, wherein said content data further includes certificate validity data concerning at least one of:

a date range identifying the period over which the certificate is valid:

the location of a certificate revocation list that should be checked before the certificate is used;

the location where a one-time use permission can be obtained or the certificate re-validated;

said content data being structured into fields with the validity data and said condition or conditions being held in the same field.

10. A computer-readable medium according to claim 1, wherein the certificate has substantially the same form as an SPKI certificate data structure with said condition or conditions being held in a validity field of the certificate data structure.

11. Apparatus for generating an electronic certificate data structure, the apparatus comprising:

a data handling arrangement for assembling content data specifying an attribute delegation from an identified issuer to a certificate subject, and including a condition requiring that a particular subject must have a particular attribute in order for the delegation to be valid; and

a signature arrangement for generating an electronic signature of said issuer over said content data.

12. – 13. (cancelled)

14. Apparatus according to claim 11, wherein the data handling arrangement is arranged to cause said certificate subject to be specifically identified in the content data.

15. Apparatus according to claim 14, wherein the data handling arrangement is arranged to cause said particular subject to be implicitly specified in said content data as said specifically-identified certificate subject.

16. Apparatus according to claim 14, wherein the data handling arrangement is arranged to cause said particular subject to be explicitly identified in the content data.

17. Apparatus according to claim 11, wherein the data handling arrangement is adapted to permit multiple said conditions to be included in the content data in predetermined logical relationship.

18. Apparatus according to claim 11, wherein the data handling arrangement is arranged to organize said content data into substantially the same form as an SPKI certificate data structure with said condition being held in a validity field of the certificate data structure.

19. A reduction engine for verifying the existence of a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said reduction engine comprising:

a trust-chain verifier for combining justified attribute delegations to form said trust chain, at least one said attribute delegation being justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain verifier to establish a branch of said trust chain upon the trust-chain verifier using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

20. A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure in which said certificate subject is specifically identified in the content data.

21. A reduction engine according to claim 20, adapted to handle a said conditional certificate data structure in which said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

22. A reduction engine according to claim 20, adapted to handle a said conditional certificate data structure in which said particular subject is explicitly identified.

23. A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure including multiple said conditions in predetermined logical relationship.

24. A reduction engine according to claim 19, adapted to handle a said conditional certificate data structure that has substantially the same form as an SPKI certificate with said condition being held in a validity field of the certificate.

25. A trust chain discovery engine for finding a trust chain of justified attribute delegations that overall imparts a required attribute from a trusted issuer to a target subject, said discovery engine comprising:

a trust-chain builder for seeking to build up said trust chain using justified attribute delegations at least one of which is justified on the basis of a certificate data structure that comprises content data bestowing a specified attribute from an identified issuer to a certificate subject, and an electronic signature of said issuer over the content data; and

a trust-chain branch control arranged to require the trust-chain builder to seek to build a branch of said trust chain upon the trust-chain builder using in the trust chain a said attribute delegation that is justified on the basis of a conditional said certificate data structure that includes in its content data a condition requiring that a particular subject must have a particular attribute in order for the delegation justified by the certificate to be valid, said branch being required to impart said particular attribute to said particular subject from said trusted issuer or another trusted issuer.

26. A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure in which said certificate subject is specifically identified in the content data.

27. A trust chain discovery engine according to claim 26, adapted to handle a said conditional certificate data structure in which said particular subject is not separately specified but is implicitly said specifically-identified certificate subject.

28. A trust chain discovery engine according to claim 26, adapted to handle a said conditional certificate data structure in which said particular subject is explicitly identified.

29. A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure including multiple said conditions in predetermined logical relationship.

30. A trust chain discovery engine according to claim 25, adapted to handle a said conditional certificate data structure that has substantially the same form as an SPKI certificate with said condition being held in a validity field of the certificate.

NONE.

NONE.